

區塊鏈與法律

程式碼之治

Blockchain and the Law:
The Rule of Code

Primavera De Filippi 著
Aaron Wright

王延川 譯
徐珮菱 校訂

聯合推薦

丁道勤 京東集團法律研究院院長 | 王文宇 臺灣大學法律學院教授
司曉 騰訊研究院院長 | 利明猷 中國信託商業銀行副董事長
谷月涵 前花旗環球證券董事長兼台灣區研究部主管
武永生 銘傳大學財金法律系教授 | 於興中 康乃爾大學法學院教授
施光訓 中信金融管理學院校長 | 葉林 中國人民大學法學院教授
趙軍 360公司法律研究院總監 | 謝哲勝 台灣法學基金會董事長



購書請上：<http://www.angle.com.tw/Book.asp?BKID=10520>

區塊鏈與法律 程式碼之治

**BLOCKCHAIN AND THE LAW:
THE RULE OF CODE**

Primavera De Filippi, Aaron Wright 著

王延川 譯

徐珮菱 校訂

 元照出版公司
元照出版 搶先試閱版

謝 辭

作者要感謝Yochai Benkler、Daniele Bourcier、Lewis Cohen、John Dahaner、Brett Frischmann、Joi Ito, Kieren James-Lubin、Lawrence Lessig、Joseph Lubin、Patrick Murck、David Roon、Jeanne Schroeder、Harald Stieber、Don Tapscott、Pindar Wong和Jonathan Zittrain給予的有益反饋和指導。作者還要感謝Rachel Epstein和Walter Beller-Morales給予的第一流研究支持，在草稿撰寫過程中，感謝COALA網絡那些努力講解區塊鏈技術知識的成員，以及那些提供支持、建議和反饋的成員，感謝Vitalik Buterin帶給我們的靈感。

Primavera De Filippi還要進一步感謝Constance Choi和Vlad Zamfir在精神和智識上給予的無盡支持，感謝Samer Hassan給予持續鼓勵，感謝Matan Field的想像力、激情和堅韌，以及哈佛大學伯克曼克萊因中心所有成員一直以來的建議。

最後，Wright要感謝妻子Alissa以及孩子Aviva和Joshua給予堅定的愛和支持。



聯合推薦

(依姓氏筆畫順序排列)

【京東集團法律研究院院長／丁道勤

互聯網起源和興起最初是資訊生產傳播的民主化，隨著網路資訊生產傳播日益中心化、集中化不斷刺激了資訊生產力的解放，但囿於網路使用者注意力有限，使得越來越多訊息資源彙聚到更集中的少數大平台，平台的自我強化促使平台經濟的崛起。而現階段似乎又開始回歸互聯網的本源，進入促進和支持高度自治系統的區塊鏈這一社會基礎設施時代。區塊鏈正重新定義現代社會的基本系統和機構，也對各國的監管和法律法規帶來衝擊和挑戰。《區塊鏈與法律：程式碼之治》介紹了區塊鏈的詳細歷史和技術發展，分析了區塊鏈對法律、現有社會和政治機構的影響和挑戰，最後提出相關的監管建議，內容詳實，體系嚴密，相信將為監管部門和行業人員提供有益參考！

【臺灣大學法律學院教授兼

公共政策與法律研究中心主任／王文字

區塊鏈技術具備去中心化特性，已對生活帶來衝擊，近年的比特幣就是佳例。此技術不但安全且有利參與，未來對國家與社會的影響將更為深遠，從智慧契約的交易模式，到自治組織的民主機制，不一而足，亟需形成新思維與新規則以為因應。本書深入探討區塊鏈與法律的關係，並提出發人深省的觀察與建議，值得大力推薦。



元照出版

搶先試閱版

■騰訊研究院院長／司 曉

從巴洛的賽博格空間獨立宣言到萊斯格的程式碼即法律，以技術實現網路自治的烏托邦主義一直備受追捧。區塊鏈技術的防竄改性、彈性和不可否認性看起來讓我們離這個目標越來越近，非常難得作者在認同這一浪潮的同時保有克制的理性，完全的去政府去中心化只存在於理論模型中，可監管的區塊鏈，相對的去中心化才是大概率的未來。

■中國信託商業銀行副董事長／利明猷

區塊鏈彷彿是第四次工業革命的巨輪，所行之處幾乎已將中央管制思維夷為平地。大家都在看，去中心化的區塊鏈技術能否為人民帶來劃時代、造福經濟社會的革命性進步。本書作者為法律跨足創新科技的頂尖專家，從各種產業角度深入解析如何應用區塊鏈，更是首本將區塊鏈與法律密切結合的權威著作，提供了法學與信任機器兩者和平共生、相輔相成的方法，引人入勝，值得推薦！



元照出版

搶先試閱版

|前花旗環球證券董事長兼台灣區研究部主管／谷月涵

區塊鏈的本質是信任機器，作者帶領我們穿梭於新舊信賴機制的歷史並展望未來，互聯網世界由於區塊鏈而創造出新價值，卻也挑戰傳統法律的管制思想。本書內容兼具廣度與深度，以穿透式又清晰的法律見解，徹底改變你我對未來秩序的想像。

|銘傳大學財金法律系教授、 企業暨金融法研究中心主任／武永生

本書作者根據區塊鏈技術：去中心化、加密、不可竄改……等特徵，基於法律觀點，在令人既期待其前瞻展望，又擔恐其監管失靈之情懷下，兼從宏觀與微觀的視角，輔以歷史洪流軌跡與具體案例，透過全面、深入、仔細的論述，為讀者提供了一本精彩的論著。「必讀」應該是對之評介最直接與適切的用詞。

|康乃爾大學法學院教授／於興中

本書以簡明求實的文風對區塊鏈技術的強大功能和局限性，及它與法律的關係作了深入淺出的論述，既有精深的理論探討，又有現實的道德關懷。對欲認真瞭解當今世界技術生態系統的人而言，是一本必讀之作。但它同時也是一本寫給大眾的基礎教材，因而適合所有人閱讀。



元照出版

搶先試閱版

| 中信金融管理學院校長／施光訓

區塊鏈技術已從數位貨幣擴展應用於全世界的商業交易，乃至一切行為。在法律主宰的秩序裡，本書作者精彩論述去中心化科技與中央管制衡平之途徑，為深刻優質的絕佳之作。

| 360公司法律研究院總監／趙 軍

區塊鏈如同本書所提到的「幽靈」一般，突破了許多政府、法律的慣常治理手段，帶給我們很多挑戰。但是，此一技術存在給社會、經濟發展以及法律關係的建立、更正和消滅所帶來的促進和便利作用不可忽視。

本書立意既嚴謹又革新：一方面，透過本書可以客觀地瞭解區塊鏈的來龍去脈、技術特點，應用場景，及其對社會、經濟與法律帶來的積極和消極雙重影響；另一方面，本書所提出的監管思路和治理思路帶給我們更多啟發，非常值得政府監管部門，研究新技術發展、政策及法規新動向的專業人士參考借鑑。

「梅花香自苦寒來」感謝王延川教授的敬業與付出，讓我們有幸全方位地瞭解一個不再神秘的「區塊鏈」。

| 台灣法學基金會董事長／謝哲勝

區塊鏈、智慧合約與人工智能已衝擊經濟世界，本書說明法律如何適當地在這場時代變革中扮演好角色，充滿創新的思維，值得推薦！



元照出版

搶先試閱版

推薦序

區塊鏈是作為一種目的型技術形態而出現的，它日漸深刻地影響著貿易、物流、金融等諸多行業，卻未滲透到現有法學研究中。這首先是由於區塊鏈的強烈技術屬性所導致的。迄今為止，區塊鏈支持者尚未提供充分的論據，說明區塊鏈在技術方面是安全可靠的。即使區塊鏈是更安全的技術工具，即使區塊鏈技術與安全加密法相輔相成，但在缺少法律規範支撐的環境下，區塊鏈交易卻未必更為安全。其次，區塊鏈技術已經初步形成了自己的語言系統，不願意或難以進入法學研究者習慣的語言系統中，因此生成了一種獨特的障礙。在該技術領域中，區塊鏈、比特幣、去中心化、智能合約等獨特術語是晦澀難懂的，它們尚未與法律術語實現有效兼容。最後，區塊鏈及其交易帶有明顯的跨國界性，與傳統法律的固有地域性或國別性形成巨大反差。區塊鏈支持者崇尚「程式碼之治」而非「法律之治」，更是形成了與既有法律秩序之間的巨大鴻溝。因此，究竟是區塊鏈在法律之外形成一個獨立的治理領地，或是區塊鏈融入現有法治、現有法治接納區塊鏈，將是區塊鏈與法律長期博弈的過程。

《區塊鏈與法律：程式碼之治》是一本有非常價值的著作。它扼要介紹了區塊鏈中若干重大話題的來龍去脈，系統地描述了區塊鏈、智能合約、比特幣、去中心化等技



元照出版

搶先試閱版

術詞語的要義，讓看似零散的技術詞語在簡要的歷史回顧中融為一體，讓法學研究者大體瞭解技術研究者的所思所想。這在迄今為止的著作中確係難能可貴的佳作。在普及區塊鏈的基礎上，這本著作從三個角度探討了區塊鏈與法律的關係，即區塊鏈在金融和合約中的應用、區塊鏈與訊息保護的關係、區塊鏈的特殊治理模式。先前我在傳統法學研究之餘，有幸被諸多年輕學者拉攏，也粗略地瞭解區塊鏈衍生出的法律問題，相信這本著作所列問題是其中的最核心問題。

通讀全文，作者揭示了區塊鏈支持者的技術信仰，這是難能可貴的。我們信仰的究竟是什麼？這是讀過全文後的一個疑問。科技的確具有改變世界的能力，然而，是否每一項新的、重大的科技都會改變世界和現有的法律秩序？世界和現有法律秩序是否願意為某項科技的出現而作出自身改變，這是值得懷疑的。若說區塊鏈是將某種人類語言轉化成某種程序化語言，若真如同作者所說的「智能合約」只是「如同法律契約的智能合約」，這似乎不足以顛覆法律反映了人與人之間關係的社會認知。作者分析了「共識機制」在區塊鏈中的價值，這是非常有趣也是有意義的。但當我們將這種「共識機制」解釋為投票機制或者共同決定機制時，似乎仍可以將區塊鏈融入既有的法律秩序，而不至於造成科技與法律的嚴重衝突。或許是路徑依賴使然，法學研究者在秉持自由之法律價值的同時，無法忽略公法的介入與干預；或許是傳統秩序的影響，人們更



相信那些可以融入秩序的自由和法治。現在宣稱「程式碼之治」具有了統治力，或許言過其實或言之過早。

海峽兩岸的區塊鏈法學研究者甚少，深入其中者更是寥寥無幾，多數法學研究者視其為畏途。王延川教授數年前即取得中國人民大學的法學博士學位，在商法研究上本就頗有建樹，現在區塊鏈與法律的域外專著中遴選《區塊鏈與法律：程式碼之治》並翻譯成中譯本，我相信這是法學界的巨大貢獻，也相信這將極大推動海峽兩岸區塊鏈法學的深入研究。受王延川教授囑託，撰寫此一推薦，深感榮幸！

中國人民大學法學院教授
中國商法學研究會副會長

葉 林

2019年1月16日於北京



元照出版

搶先試閱版

購書請上：<http://www.angle.com.tw/Book.asp?BKID=10520>



元照出版

搶先試閱版

序 文

從「人的治理」到「機器的治理」

現代社會日益複雜，社會治理日漸成為最重要的議題。如何才能實現社會的良性治理？有人說依靠國家法律，也有人說依靠倫理和道德。這兩種說法固然正確。但對於治理的對象即活生生的人而言，這種外部規制始終過於表面化，缺少必要的中間環節。換個角度理解，社會良性治理呈現為人們和諧生活，這種和諧來自於人們內心的確信，這個由內而外的確信即為信任，來自於交流對象彼此行為效果的可以預期。因此，正確的說法應該是，並非規則實現了社會治理，而是人與人之間基於信任實現了社會治理，規則只是在一定程度上提升或者降低該種信任，穩固、提升或減損了社會治理的效果。在缺少信任的社會環境中，規則非但難以促使人們良性互動，且會成為一種破壞人們良性互動的工具。故規則按照此邏輯發揮作用：人們預測互相交流的對方也會服從自己服從的規則，基於此種認識，人們彼此相信對方，和諧生活。規則背後另有一種規範。所以，埃里克森認為，「是規範，而非法律規則，才是權利的根本來源」¹亦即，規範是本，而法律規則

¹ [美]埃里克森：《無需法律的秩序》，蘇力譯，中國政法大學出版社2004年版，第63頁。



是表。這裡的規範主要是指社會規範，表現為人與人之間的信任規則。韋克伯格描述了倫敦鑽石商人的交易情形：「在鑽石街上，人們從事著價值數十萬英鎊的鑽石交易。在黑暗的小屋裡，商人甲向乙出售幾顆昂貴的寶石，生意很快就談妥了，甲揚長而去，乙俯身仔細檢查那些寶石。他們之間沒有契約，沒有任何書面文件，一切交易都透過口頭完成」。²這種交易背後則是信任作為支持。從這個角度而言，信任是經濟交易乃至於社會交流的基石。

關於信任的作用，許多著作均有所涉及。³目前主流觀點認為，信任屬社會資本，作為潤滑社會交流關係的善意儲備，可以增加整個社會的財富，反之，若缺乏信任，社會互動關係將會演變成囚徒困境（prisoners' dilemma），非但不能提升效率，且會造成資源的極大浪費。近來美國學者凱文·韋巴赫提出了信任架構（trust architectures）概念，⁴對我們理解信任的產生以及社會治理有很大幫助。在韋巴赫看來，信任是一種架構，具有其得以催生的原點和輻射的範圍。他按此標準將信任架構區分為三種：利維坦

² [美]詹姆斯·科爾曼：《社會理論的基礎（上）》，鄧方譯，社會科學文獻出版社1999年版，第128頁。

³ 參見[美]弗朗西斯·福山：《信任：社會美德與創造經濟繁榮》，海南出版社年版。[德]尼克拉斯·盧曼：《信任》，上海人民出版社2005年版。[法]阿蘭·佩雷菲特：《信任社會》，商務印書館2005年版。鄭也夫：《信任論》，中信出版集團股份有限公司2015年版。

⁴ 本人對此的理解就是自帶規則的信任，或者說信任由規則而支持和維持。



（Leviathan）⁵信任架構、點對點（peer-to-peer）⁶信任架構和無需信任的信任（Trustless Trust）架構。⁷

「利維坦信任架構」是指以中央機構為原點而形成的信任架構，民眾由於信任中央機構而進行社會交流。例如，我們信任不動產登記機關的權威，進而放心透過其對不動產信息記錄來公示產權。我們信任銀行的權威，進而放心透過其對匯兌和支付信息進行記錄來表示貨幣的移轉。我們信任法院，進而放心將我們與別人的糾紛交由其進行裁決，並遵守其作出的裁判結果。民眾之所以對中央機構有此信任，乃因其背後有國家強力支撐，若違背了該信任架構，違背者會受到懲罰。正是由於此種信任架構的明確性與可預期性，以及賞罰分明措施，其可輻射至一國的地域全境。此普遍化的信任架構亦是目前國際上最主流的社會交流治理模式。

利維坦式信任架構的典型例子是以股票交易為核心建立起來的資本市場。資本市場的特質決定了政府機構的高度介入。首先，在資本市場中，金融機構主要使用「別人的錢」進行投資，所以，其中的交易基本上屬代理關係，

⁵ 該詞語出自於英國啟蒙時代哲學家托馬斯·霍布斯的著作《利維坦》，「Leviathan」原意為裂縫，在《聖經》中象徵邪惡的一種海怪，在霍布斯的著作中，其意指近代以來經過社會契約而形成的巨大的國家機構。

⁶ Elinor Ostrom將這樣的架構稱為公共池資源治理的設計原則（design principles for governance of common-pool resources）。

⁷ See Kevin Werbach, Trustless Trust, <http://ssrn.com/abstract=2844409>.



容易誘發機會主義風險。其次，在資本市場中，交易雙方都需要知道對方的詳盡訊息，信息披露成為交易的核心要求。最後，資本市場具有系統性風險，一旦出現問題，不僅會影響國內資本市場之外其他經濟領域，甚至會影響其他國家的資本市場安全。上述問題無法透過交易者達成聯盟而解決，亦無法透過法院的事後介入加以解決，只能透過發揮中央政府的事前監管作用而解決。⁸

信任中央機構衍生的社會交流存在一些問題：第一，由中央機構保管的官方交流紀錄可能會出錯，第二，維持官方交流紀錄需要花費高昂成本。人們之所以放心和陌生人進行交易，是因為一般都相信銀行和產權登記機關保管的交流紀錄不會出錯。但事實並非如此，除了中央機構職員有意竄改之外，交流紀錄也會出現其他的錯誤情形，若交易方與中央機構各以自己的方式對紀錄進行判斷，就會產生糾紛。例如，某個人的銀行資產記載餘額為1,000元，而個人主張其真實帳戶餘額為10,000元，雙方爭執不下。為了得到公正結果，可以去銀行內部申訴，但是層級處理是銀行管理的要求，需要經過許多層級審批，最後或許可以找到解決糾紛的出口，但這將是一個漫長的過程。各種流水單以及存款是否被人提取，自動提款機的提取紀錄等，這一切都需要被證明。若內部解決不暢，需要第三方介入。例如，雙方可訴諸於法院，但司法程序更是繁瑣無

⁸ 參見[美]拉古拉邁·拉詹、路易吉·津加萊斯：《從資本家手中拯救資本主義》，中信出版社2004年版，第126-131頁。



比，即使讓職業律師介入，也需花費很高的時間成本。為了維持交流紀錄，防止紀錄滅失，中央機構需要電子備份，為了防止電子系統遭受駭客入侵等危險發生，甚至需要進行紙本備份，並將其保存在一個極其安全的地方，而這些保存成本非常高昂。

「點對點信任架構」是希望能夠消除中央機構消極作用的一種嘗試。它是指基於我們對長期互動而產生的人際關係和共同社區規範的信任而產生的信任架構。在該信任架構裡，相互信任的人之間具有共同的交流背景（background），信守自己群體自創的交往規則，即勞倫斯·萊斯格所說的社會規則（social norms），這種自覺意識在一定程度上消解了中央機構的作用。⁹交流者彼此之間相信對方不會破壞規則，例如在雞尾酒會上，你偶爾失禮，但相信對方的涵養不會和你計較，讓你難堪。我相信你，並非因為有中央機構的存在，而是因為我信任你這個人。基於此，中央機構被排除在信任架構之外，個體的人而非抽象的中央機構成為信任的原點。

點對點信任架構最著名的例子就是中世紀商人們構造起來的交流網絡。該網絡的目的在於排斥中世紀各種權威機構對於商人之間交流的介入。關於商人之間交流關係的規範，不再依靠王室制定的法律，而是依靠商人之間心照

⁹ See Lawrence Lessig, Code: And Other Laws of Cyberspace, Version 2.03, Basic Books (2nd ed. 2006).



不宣的某種社會規則，「商人間實行合作，不論採用什麼形式，都需要忠誠、信任、以及恪遵指令。由此形成一種相當嚴格的商業道德。」¹⁰這也是Elinor Ostrom、Robert Ellickson和其他人發掘到的公共管理（commons regimes）領域，在那裡無需法律也可以實現社會秩序。¹¹對於當事人之間的交流而言，良好表達的社會規範和標準，加上人們對自身聲譽的珍視足矣。後來，商人們將這些規範和標準整理，制定成僅適用於自身的所謂商人法（Law Merchant）。「商人們自發聚集在一起，制訂共同的遊戲規則。商業法律由此誕生。它沒有得到國家的承認，完全是自發產生，自行裁決並強制實施，就像一個俱樂部的規章制度一樣。」¹²商人不僅創制規則，而且建立了執行該規則的機構，「商人組建自己的法庭來執行源於自願合同交易的自設法律框架。」¹³這種規則雖然是一種軟規範，但商人

¹⁰ [法]布羅代爾：《15至18世紀的物質文明、經濟和資本主義：形形色色的交換（第二卷）》，顧良譯，生活·讀書·新知三聯書店1993年版，第143頁。

¹¹ See Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*, *Political Economy of Institutions and Decisions* (1990); Robert C. Ellickson, *Order without Law: How Neighbors Settle Disputes*, Harvard University Press (1991).

¹² [美]麥特·里德雷：《美德的起源：人類本能與協作的進化》，劉珩譯，中央編譯出版社2004年版，第221頁。

¹³ See Leon E. Trakman, *From the Medieval Law Merchant to E-Merchant Law*, 53 U. TORONTO L.J. 274 (2003) see also Robert D. Cooter, *Decentralized Law for A Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1647 (1996).



們輕易不敢違反，否則將會被孤立，寸步難行。¹⁴在14世紀的義大利，身處商事交易市場中，「任何人，若沒有履行他在集市開市期間所簽訂的協議，都被認為是名譽掃地之人。他將完全喪失了自己的信用，再也無臉參加集市。」¹⁵

基於點對點信任架構建立起來的交流網絡也有弱點：第一，不像利維坦信任架構那樣，點對點信任架構的輻射範圍有限，基於此而構建起來的社會交流網絡半徑不夠寬廣。因為若脫離開某種個體或者某種文化背景，特定的信任架構就可能失效。例如，中國傳統社會的宗族信任就屬於點對點信任架構，超出宗族的人們之間不會產生信任。地區商會也是如此，其成員之間可以相互信任，超出該圈子則很難自動產生信任。第二，它依靠經常瞬息變化的社會聯繫和非正式治理結構。若人們之間的社會聯繫降低，則信任架構就會發生變化，或者產生轉向。例如，社區中突然有些人不願意再信任社區規則，如果範圍較小，社區會進行矯正，如果範圍逐漸擴大，本應信守規則的人會認為繼續信守規則反而對自己不利，透過理性考慮後，他也可能會選擇破壞規則。所以，信任架構非常脆弱，用Diego Gambetta的話來說，「信任是相互關聯（relevant）的，往

¹⁴ 參見王延川：《現代商法的生成：交易模型與價值構造》，法律出版社2015年版，第39-42頁。

¹⁵ [英]彼得·斯坦、約翰·香德：《西方社會的法律價值》，王獻平譯，中國人民公安大學出版社1989年版，第283頁，註1。



往伴隨著退出、出賣、背叛的可能性。」¹⁶追根溯源，是因為信任是「無追索權的信賴（reliance without recourse）。」¹⁷因此，沒有強力支持，難以成就良性的社會治理。

到目前為止，世界範圍之內，社會治理主要依賴這二種信任架構，二者雖然邏輯有差異，本質上卻相同：都屬人對人的治理。因為利維坦信任架構中，中央機構執行者往往由自然人擔當。點對點架構中，也是將信任原點置於具體的自然人身上。由於是人對人的治理，最後難免受到作為執行者或者被信賴者的人之機會主義行動傾向的影響。

區塊鏈的出現，為社會治理提供了第三種信任架構：無需信任的信任架構。即透過加密技術與分散式共識網路得以實施。這種新的範本讓信任系統輸出成為可能，交流網絡的形成並不需要其中的任何行動者。區塊鏈透過技術建立起來的信任架構可以超越上述兩種信任架構：首先，交流者不再依賴於中央機構，信任點不在於中心，而是去中心，具體表現為分散式節點，而且這些節點是透過協商表決的方式實現。其次，交流者也不再信賴相對的行動者，該架構的特點不再留停在對交流對象的信任上，而是超越了對人的信任，因此成為無需信任的信任。最後，該

¹⁶ See Diego Gambetta, Can We Trust?, in Trust: Making and Breaking Cooperative Relations (Diego Gambetta ed., 1988): 218-219.

¹⁷ See Gus Hurwitz, Trust and Online Interaction, 161 U. PENN. L. REV. 1579, 1584 (2013).



信任架構建立起來的交流網絡可以超越其他兩種信任架構建立起來交流網絡。理論上而言，基於區塊鏈的交流網絡可以足夠廣大，達到超乎想像的程度。凡是使用區塊鏈APP的用戶，無論身處何地，身分為何，都會形成交流網絡。所以，它的信任範圍可以超越國界和某種緊密的共同體。

無需信任的信任架構的典型例子是智慧合約。智慧合約表現為一段程式碼，如果程式碼預先設定的條件滿足，就會被嵌入區塊鏈中，程式碼中記載的交易者意圖被自動執行。與傳統合約不同的是，程式碼一旦運行不得被停止或者修改，杜絕了交易者的機會主義行為。由於區塊鏈底層協議的精神是「程式碼即法律」，因此，借助於區塊鏈，智慧合約排除了第三方在交易中的自由裁量權，其目的在於打造一個獨立的「法外世界」。基於區塊鏈，人們不再信賴權威機構，只要相信帶有程式碼與演算法的機器即可。¹⁸

基於其分布式共識演算法，區塊鏈在一系列行業可以開闢新的可能性。¹⁹區塊鏈正在建構一個無需信任的交流體

¹⁸ 「重要的規則，不是透過社會制裁，也不是透過國家，而是透過特定空間的架構強加的。一個規則不是透過法規來定義的，而是透過管理空間的程式碼來定義的。」 Lawrence Lessig, *Code: And Other Laws of Cyberspace*, Version 2.03, Basic Books (2nd ed. 2006).

¹⁹ See Michael Casey, *Blockchain Technology: Redefining Trust for a Global, Digital Economy*, LINKEDIN PULSE (June 13, 2016), <https://www.linkedin.com/pulse/blockchaintechnology-redefining-trust-global-digital-michael-casey>.



系：作為區塊鏈1.0的比特幣主要應用在在支付領域。作為區塊鏈2.0的智慧合約主要應用在全球支付、銀行貸款、抵押品管理、代理投票、證券發行以及監管和合法活動以及創建分散式自治組織。作為區塊鏈3.0的處理系統主要應用在社會治理領域，包括身分認證、公證、仲裁、審計、域名、物流、醫療、郵件、簽證、投票等領域。如果照此發展下去，未來各行各業都可以利用區塊鏈建構自己的交流網路，使得無需信任的信任架構成為社會生活的重要基石。

無需信任的信任架構透過機器在人們之間形成交流關係，人們透過對機器的信任取代了對中央機構和交流相對人的信任，正因如此，《經濟學家》雜誌用「信任機器」（Trust Machine）為區塊鏈命名。²⁰而建立在區塊鏈信任架構基礎上的社會治理就是「機器的治理」。正是因為機器的確定性與不可竄改性，使得未來的交流網路擺脫了機會主義和不確定性等影響，促進了良性的社會治理。但是，也有人提出異議，認為信任是一個被信任的人的善意表現。而機器沒有意志，因此，機器不能被信任。²¹另外，區塊鏈的確可以實現交流的確定性與不可竄改性，但是，這

²⁰ See The Trust Machine, *ECONOMIST* (Oct. 31, 2015), <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-couldtransform-how-economy-works-trust-machine>. See also Adriano and Monroe, *The Internet of Trust*, *FINANCE & DEVELOPMENT*, June 2016, <http://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm>.

²¹ See Karen Jones, *Trust as an Affective Attitude*, 107 *ETHICS* 4 (1996): 5-6.



種優勢既可以服務於善的目的，也可以服務於惡的目的。例如，智慧合約可以成為正常社會交易的重要手段，同時也成為洗錢、賭博、恐怖組織融資以及暗殺的絕好工具。²²

有學者提出了較為中肯的觀點，「密碼學和軟體可以取代守門人，但這並不意味著我們完全不相信人類。」²³無需信任的信任的起點和終點都是人，活生生的自然人。而人之最重要的社會價值即是自由，演算法和機器的確可以導致一個高度定制性和確定性秩序的形成，這個秩序可以消除機會主義和各種人力所導致的混亂，從而提升社會效率。但是，這種高度定制性和確定性秩序在一定程度上會消解自由。因為人們借助於區塊鏈作出選擇之後，不得偏離程式碼即法律這一鐵律，從這樣意義上而言，人們之間的交流被其下層的技術程式碼所自動強制執行，而不再顧及各交流方的意願。程式碼即法律不可能容忍錯誤，即當程式碼承載的並非交流者的真意，或者距離交流者的真意有差距時，程式碼依然強制執行，所以，依託於區塊鏈，從追求確定性的目標走向不正義的確定性目標。

²² 有研究表明，透過智慧合約可以控制的賞金，暗殺一名公眾人物，並透過預言機進行驗證。See Ari Juels, Ahmed Kosba and Elaine Shi, The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (New York: ACM, 2016): 283-295.

²³ See Pete Rizzo, Circle Execs: The DAO Proves Blockchains Require Trust, CoinDesk (June 22, 2016, 3:09 BST), <http://www.coindesk.com/circle-execs-dao-proves-blockchaintrust/>.



區塊鏈的核心理念是「去中心化」，透過技術排除中介機構的干預，交易者不再需要信任中央機構，而只需要信任機器足矣。同時，區塊鏈的運行也是無邊界的，可以揚棄點對點信任架構的輻射限制。但這只是理想主義的，這樣下去會產生所謂的「技術偏見」（Technical prejudice）和「演算法霸權」（Algorithm hegemony）。就像本書作者在一篇論文中揭示的那樣：「演算法治理可能最終導致一個高度規定性和確定性的系統；人們的確可以自由地決定他們想要遵守的特定規範集，但是在作出選擇之後，不得偏離這些規則，從這樣意義上而言，智慧合約被其下層的技術程式碼所自動強制執行，而不顧各方的意願。」²⁴

即使區塊鏈得到廣泛部署，政府和利益集團依然不會輕易離場，而是會在靜觀技術發展之後尋找介入的契機，從而享受技術創新帶來的成果。在我們的人類基因中，始終難以逃脫管制這一因素，這一方面表現為我們需要被管制，另一方面權威機構想要管制我們。在中世紀，切實履行承諾成為一種交易共識，在很長一段時間內，這種共識的獲得靠的是商人之間的信任和自律，以及建立在該信任和自律基礎上的自治規範，但是發展到後來，第三方譬如地方王侯對商人交易的介入也不可避免。²⁵當初互聯網崛起

²⁴ See Aaron Wright and Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, <http://ssrn.com/abstract=2580664>.

²⁵ 參見王延川：《現代商法的生成：交易模型與價值構造》，法律出版



之時，許多人就樂觀地認為世界會發生兩大變化：第一，中介機構介入人們生活的時代已經結束，第二，超越國家地理邊界的交流將會形成。但是，實際上，就像學者研究結果顯示的那樣：第一，互聯網的興起並沒有消除中介，而只是改變了它們的形式。它創建了一大批新中介，其中最重要的是互聯網服務供應商、搜尋引擎、瀏覽器、物理網絡等，「簡而言之，互聯網使網路本身成為許多行為的中介，在互聯網之前我們可能以為根本就沒有中介。」²⁶第二，互聯網並沒有產生一個全球性的無邊界網路，而是「國家網路的一個集合——仍然透過互聯網協議連接的網絡，但為了許多目的而被分開。」²⁷

因此，無論是區塊鏈本身存在的問題，還是中央機構的既得利益問題，未來的結果肯定是區塊鏈接受政府的監管，程式碼之治與法律之治聯手，這是本書作者的主要觀點。就現有的研究而言，這是一種遠見卓識。

社會學家林·札克把人類社會的信任分為三種：一是基於血緣、基於身分的信任；二是基於歷史、基於瞭解的信任；三是基於制度的信任。第三種信任在前二者基礎上而產生的更為進步的信任。顯然，基於制度的信任是一種

社2015年版，第39-42頁。

²⁶ See Goldsmith, Jack L. and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford UP. (2006): 70.

²⁷ See Goldsmith, Jack L. and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford UP. (2006):142-161.



制約的信任和法治的信任，這種信任具有最高的可信度，也是一種普遍化的信任。借助於區塊鏈技術的信任奉行「程式碼即法律」，其可信性不亞於制度信任。如果二者強強聯手，良性社會治理指日可待。譯者進而認為，區塊鏈信任的出現不會讓目前的兩種信任架構退出歷史舞臺，相反，在未來的社會治理中，三種信任架構將同時存在，相互補充，在各自不同領域內發揮作用。但是，如何透過設計讓三種信任架構聯合起來發揮績效，是未來學者需要關注的重大課題。

王延川



元照出版

搶先試閱版

目 錄

謝 辭

聯合推薦

推薦序

葉 林

序文——從「人的治理」到「機器的治理」 王延川

引 言..... 1

第一章 技 術

一、區塊鏈、比特幣、去中心化運算平臺	13
(一)公私金鑰加密和數位簽章	14
(二)商業互聯網和點對點網路	17
(三)數位貨幣	21
(四)比特幣	25
(五)以太坊	35
(六)去中心化文件共享和覆蓋網路	40
(七)許可制的區塊鏈	42
二、區塊鏈的特徵	45
(一)去中心化與跨國性網路	46
(二)彈性和防竄改性	48
(三)透明和不可逆數據	50
(四)假 名	52
(五)激勵和成本結構	54
(六)共 識	58
(七)自 主	60



元照出版

搶先試閱版

(八)區塊鏈的雙重性質	62
(九)區塊鏈和互聯網層	64
(十)TCP/IP模型	65
(十一)區塊鏈如何適應TCP/IP模型？	67
(十二)加密安全法	69
(十三)協議和權力	75
(十四)區塊鏈技術的挑戰	80

第二章 區塊鏈、金融、合約

一、數位貨幣與去中心化支付系統	83
(一)改進付款和匯款系統	87
(二)數位貨幣和現行法律	90
(三)數位貨幣和降低的財務隱私	94
(四)可替代性和透明度	97
(五)限縮中央銀行的作用	99
二、如同法律契約的智慧合約	101
(一)智慧合約和法律契約	103
(二)混合協議	108
(三)依賴智慧合約的協議的法律強制執行力	111
(四)降低監控成本和機會主義行為風險	114
(五)程式碼的益處	115
(六)智慧合約的侷限性	118
(七)隱私問題	118
(八)法律義務的形式化	119
(九)匿名當事人之間的協議	120
(十)契約標準化	121
(十一)犯罪或不道德的合約	123



三、智慧證券及衍生性金融商品	126
(一)智慧證券	133
(二)智慧衍生性金融商品	136
(三)智慧證券及衍生產品的侷限性	138
(四)去中心化的資本市場	143

第三章 區塊鏈和資訊系統

一、防竄改、驗證和認證資料	155
(一)登記機構和公部門資訊	159
(二)經鑑證和認證紀錄	164
(三)安全風險	167
(四)垃圾進，垃圾出	169
(五)隱私遞減帶	171
二、彈性和防竄改資訊系統	173
(一)區塊鏈和去中心化資訊儲存	176
(二)基於區塊鏈的文件共享服務	177
(三)區塊鏈和防審查通訊	179
(四)互聯網域名系統	180
(五)著作權問題	182
(六)言論自由的另一面	185

第四章 組織與自動化

一、組織的未來	189
(一)公司治理和內部控制	193
(二)去中心化組織	197
(三)分散式治理模型	202
(四)安全問題	203
(五)有限責任的缺失	205



(六)證券法面臨的挑戰	207
(七)去中心化組織的不可規範性	209
二、去中心化自治組織	211
(一)定義去中心化自治組織	214
(二)自動治理的好處	218
(三)市場失靈	221
(四)法律問題	222
三、物聯鏈	225
(一)支持區塊鏈的裝置	229
(二)設備管理	232
(三)由機器促進的契約	233
(四)財產權管理系統	234
(五)解放裝置	239
(六)被解放裝置的監管問題	242

第五章 調整基於區塊鏈的去中心化系統

一、監管模式	247
(一)監管終端用戶	250
(二)傳輸層	253
(三)資訊中介機構	256
(四)區塊鏈特定中介機構	257
(五)礦工和交易處理商	259
(六)監管程式碼和架構	261
(七)硬體製造商	264
(八)監管基於區塊鏈的市場	266
(九)透過社會規範監管	268
(十)監管權衡	272



二、作為法律的程式碼	277
(一)置換法律為程式碼	280
(二)作為監管技術的區塊鏈技術	283
(三)程式碼作為法律的侷限性	287
(四)自動化規則	290
(五)定制規則	291
(六)加密安全法和演算法治理	292
結 論	295
後 記	王延川



購書請上：<http://www.angle.com.tw/Book.asp?BKID=10520>



元照出版

搶先試閱版

引言

西元1988年，「密碼龐克（cypherpunk）」運動的創始人之一蒂莫西·梅（Timothy May）警告世人：「一個幽靈正出沒在現代世界。」¹這個幽靈不是政治僵局、恐怖主義、種族衝突或環境危機。而是一種新形式無政府狀態的發展和擴張，梅將其稱之為「加密無政府狀態（cryptoanarchy）」。²正如他在「加密無政府主義宣言」中描述的那樣，互聯網和公私鑰密碼術的進步太快就會讓個人與團體相互之間以更隱密的方式通訊和互動。依靠不可追蹤的網路和「防竄改盒實施加密協議」，人們將會獲得「經營商業，及在不知對方真實姓名或法律地位情況下協商電子契約」的能力。³

最後，梅預測，個人將從國家中解放，徹底改變「政府監管的性質、稅收和控制經濟交流的能力、保持資訊隱密的能力」，以及我們關於信任和名譽的真正觀念。⁴加密圖形安全協議將拆除由智慧財產權打造的「鐵絲網」，打破資訊流動，使個人具有新的自組織能力，並改變公司和政府的性質。⁵在梅看來，這種形勢的擴散是不可避免的。正如他在其後的著作中解釋的，「精靈已從瓶中飄出」，沒有什麼可以阻擋技術性

¹ 宣言可以追溯至1988年。The manifesto dates back to 1988. See Timothy May, "The Crypto Anarchist Manifesto" (1992), <https://www.activism.net/cypherpunk/crypto-anarchy.html>.

² Ibid.

³ Ibid.

⁴ Ibid.

⁵ Ibid.



2 區塊鏈與法律：程式碼之治

無政府狀態這種不可遏止的浪潮。⁶

區塊鏈在很多方面皆是近三十年前梅所預期的「防竄改盒（tamper-proof boxes）」。⁷他們將幾種現有技術融合在一起，包括點對點網路，公私鑰加密技術和共識機制，以創建可被認為是極具彈性和防竄改的資料庫，在那裡人們能以透明和不可否認的方式儲存數據，並以假名方式（pseudonymously）從事各式各樣的經濟交易。區塊鏈正在推動數位貨幣及其他有價值資產的移轉，管理財產權益和敏感紀錄，其中可能最深刻的是，促進被稱為智慧合約（*smart contracts*）電腦程式的創建，它能夠自動執行。⁷

區塊鏈的運行與早期資料庫不同，因為它們不是集中維護的。它們由電腦〔稱為「對等點（peers）」或「節點（nodes）」〕組成的點對點網路共同管理，此些電腦通常分布在全球各地。⁸而這些節點儲存了精確或幾乎精確的區塊鏈的副本，並透過使用軟體協議進行協調，該協議精確的規定了網路參與者如何儲存資訊、參與交易以及執行軟體程式碼。

由於區塊鏈被廣泛複製，儲存在區塊鏈中的任何資料皆具有高度的彈性，即使區塊鏈的副本損壞或網路上的一個節點發生故障，仍可以繼續存在。只要區塊鏈的有效副本存在於世界某個地方，區塊鏈即可被其他人恢復並複製，以檢索過去的紀

⁶ Timothy May, “Crypto Anarchy and Virtual Communities” (1994), <http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html>.

⁷ Ibid.

⁸ 譬如，正如我們將在第一章中更詳細描述的那樣，比特幣區塊鏈目前儲存在89個轄區的6,000多台電腦中。See “Global Bitcoin Node Distribution,” Bitnodes, 21.co, <https://bitnodes.21.co/>. 另一個以區塊鏈為基礎的大型網路Ethereum擁有超過12,000個節點，也遍布全球。See Ethernodes, <https://www.ethernodes.org/network/1>.

錄並參與新的交易。

為了確保資訊的有序記錄並增強區塊鏈的安全性，每個區塊鏈都包含一個共識機制（*consensus mechanism*）——一套嚴格的規則和預先設定的激勵和成本結構——這使得任何一方很難或者需花費高昂成本去單方面刪除或修改儲存在區塊鏈上的資料。共識機制有助於基於區塊鏈的網路定期就共享資料庫的當前狀態達成一致——即使成員不瞭解或信任彼此。

透過公私鑰加密技術編排，每個區塊鏈驗證紀錄到區塊鏈數據的完整性，並使人們能夠以假名方式參與交易，而不必透露他們的真實身分。⁹因為區塊鏈不是中央維護的，沒有任何一方需要控制對它們的造訪。隱蔽來說，在公共可造訪的區塊鏈上，任何人皆可以創建一個基於區塊鏈的帳戶——由一個公共位址、一個私人金鑰和一個程式碼組成——並與他人進行交易，而不必擔心第三方的干預。¹⁰

更先進的區塊鏈還整合了分散式的運算系統——換句話說，分散式虛擬機和圖靈完備（*Turing-Complete*）的編程語言，使各方可以編寫和部署智慧合約程式。¹¹這些程式儲存於區塊鏈中，並由區塊鏈下的多位成員執行，從而創建自動的、一旦部署就很難關閉的電腦程式。

自2009年推出比特幣以來，區塊鏈支撐了一系列旨在利用該技術儲存資訊並運行電腦程式的線上服務。其中一些應用旨在滿足梅的願景，而另一些則有助於加強現有的合法服務。

正如比特幣所展示的，區塊鏈技術支持去中心化、全球性的價值移轉系統，該系統既是跨國的，又是匿名的。使用區塊

⁹ Ibid.

¹⁰ 有些區塊鏈不能公開造訪（更多資訊請參見第一章）。這些區塊鏈被稱為「私有區塊鏈」，但並不是本書討論的重點。

¹¹ 參見第一章。

4 區塊鏈與法律：程式碼之治

鏈，任何人都可以交換數位貨幣，如比特幣或其他有價值的資產，而無需依賴中央結算所，也不需揭露他們的身分。區塊鏈是新穎的點對點匯款系統的底層技術，降低了向國外匯款的成本，並使該技術在金融服務行業中占據一席之地，為新的分散式系統提供動力，而這些系統衝擊著全球金融的核心，包括去中心化的證券和衍生性金融商品交易。

在短短幾年的時間裡，區塊鏈覆蓋範圍迅速擴大，不再侷限於支付系統和金融產品，更有助於支持建構社會和經濟互動的新型自治系統，該系統對中央機構之需求較少。智慧合約正被用於記錄全部或部分法律協議，創造動態且可能更難終止的商業安排。

全球各地的政府正在試驗區塊鏈，以確保和管理關鍵的公共紀錄，其中包括重要資訊和權益或財產契約。透過利用區塊鏈的防竄改性、彈性和不可否認性，政府希望能高度保證關鍵資訊的完整性和真實性。隨著時間的推移，區塊鏈可以鎖定新的公共基礎設施，甚至可能鎖定全球和跨國系統，任何人皆可透過網際網路連接加以使用。

區塊鏈也開始建構集體活動，包括（少部分的）透過密碼管理新型數位組織。由於區塊鏈可以廣泛被造訪並可促進經濟交易，因此它們正被探索如何管理現有法律實體的運作，作為協調的中心點，透過智慧合約實施基於密碼的規則，可以降低管理團隊活動的成本和難度。區塊鏈甚至正為更透明、更少級別化的新型組織提供動力，幫助不同群體中彼此不瞭解的個人間達成協議。由於區塊鏈能夠執行自治程式碼，並隨著時間推移，還可提供基礎架構來創建完全依賴於演算法系統和人工智慧（AI）管理團隊活動的組織。這些組織不會依賴人工進行管理，而是依靠基於程式碼的規則和其他演算法治理手段來建構其運行。



除了潛在的協調人類活動之外，區塊鏈日益被用於控制設備和機器，並透過智慧合約來界定這些基於網際網路連接設備的運行。最終，區塊鏈可能會發展成一個基礎層，幫助機器、人類以及其他機器進行經濟交易。如果這些嘗試成功，區塊鏈可能最終被用於管理越來越多的活動，從而形成機器對機器和人機互動的新時代，將可能改變我們與實物之間關係的本質。

然而，並非所有基於區塊鏈的應用和服務都嚴格遵守現有的法律和法規。以區塊鏈為動力的數位貨幣跨國運行，往往忽視目前有關貨幣傳輸和洗錢的法規（監管），以及旨在幫助政府、銀行和其他私人機構追蹤全球範圍內資金流動的法律。如果監管不善，這些新興技術可能被用來實施詐欺行為，並參與洗錢、恐怖主義融資或其他非法活動。¹²

區塊鏈也在搶占公開市場，使各方能夠透過使用基於程式碼而自主和不受監管的交易所，出售數十億美元受加密保護的「代幣（tokens）」——其中一些類似於證券——和交易衍生性商品和其他金融產品。這些基於區塊鏈的系統通常會忽略為支持現有金融市場所設置的法律障礙，並削弱旨在限制詐欺和保護投資者而精心制定的法規。

在金融領域之外，區塊鏈一直被用於支援規避線上賭博和電子商務交易限制的應用，支援不受中央機構羈絆的高度自動化賭場、支援去中心化電子商務市場，以促進不依賴eBay、克雷格名單（Craigslist），甚至絲綢之路（Silk Road）購買和出售商品。這些應用有助於促進毒品的銷售，並可在充分應用的情況下，打破政府對惡習及其他令人不悅之社交活動限制。

¹² The European Securities and Market Authority, “Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets,” ESMA/2016/773, June 2, 2016: at 17, https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf.

6 區塊鏈與法律：程式碼之治

區塊鏈進一步幫助打開資訊流，為新型的點對點文件共享應用程式、分散式通訊平臺及社交網路提供動力，這些（服務）依賴於區塊鏈和其他點對點網路的防竄改和彈性特質，以傳播受版權保護、煽動性和不雅的資料。如果被廣泛使用，這些服務可能會打擊政府及企業線上控制、過濾和審查資訊的企圖，而忽略了這可能涉及之社會與經濟成本。

如果區塊鏈在速度、性能、功能和可造訪性方面皆有所提升，那麼該技術將可能會在更長的時間範圍內開始建構與傳統企業和其他法律實體競爭的組織，甚至可能促使自主設備以及機器人的出現，並獨立於任何第三方運行——不受政府和中間營運商的控制。

正如我們在本書中表明的，區塊鏈促進支援自治系統的能力，將日益為尋求控制、塑造或影響區塊鏈技術發展的國家和監管機構帶來挑戰。如許多其他技術一樣，區塊鏈可以被部署以支援和削弱現有的法律和法規，但是該技術之所以特別強大，是因為它能夠促進全球運作的彈性、防竄改和自動化的基於程式碼系統的建構，為人們提供取代重要社會職能的新型金融和契約工具。

透過區塊鏈，人們可以建構自己的規則或智慧合約系統，由基於區塊鏈的網路協議執行。這些系統在沒有法律的情況下創建秩序，並實施可以被認為是私人監管框架的東西——我們將在本書中稱其為「加密安全法」。¹³他們賦予軟體開發人員創建工具和服務的權力，這些工具和服務規避了管轄規則，並且跨國運作以協調一系列經濟和社會活動。

¹³ 「無需法律的秩序」現象也在其他文獻中有所描述，其中最引人注目的是羅伯特·埃里克森的開創性著作《無需法律的秩序》。而該書於1994年由哈佛大學出版社出版。

加密安全法與現今基於程式碼規則由線上應用實施的現有系統不同。¹⁴目前大多數的線上服務通常不是作為中介機構，就是依靠其他中介機構——如大型雲端供應商、搜索引擎、代理收付、域名註冊商和社交網路——來支持其服務。這些中介機構有權實施和執行法律及自己的規則，並且只要它們易於識別和定位於特定的管轄區域內，則也可以作為監管機構的中心控制點。¹⁵

部署在區塊鏈上的系統——主要或完全依賴於加密安全法——將難以控制和管理。區塊鏈減少了對中介的需求，並創建了由協議和其他基於密碼的規則管理的系統，這些規則由底層的、基於區塊鏈的網路自動執行。透過使用區塊鏈和相關的智慧合約，新型線上應用可以被設計成為高度自治且日益排除中央中介機構的影響。這些應用僅由密碼組成，由基於區塊鏈的協議以去中心化方式執行——無論它們是否遵守法律而與專注於監管中央中介機構的法律體制產生緊張關係，這些中介機構目前控制或幫助促進社會和線上經濟活動。

儘管表現出很大的希望，但基於區塊鏈的網路冒著風險製造分散性風險，可能會動搖中央銀行、金融市場和商業協定的管理，並支持新形態的違法活動。這些風險尤其突出，因為這項技術正被用於重寫界定現代社會的基本系統和機構，包括存在於我們社會中的支付系統、金融市場、商業協定，以及眾多

¹⁴ 喬爾·瑞登伯格（Joel Reidenberg）使用術語「資訊法（lex informatica）」來描述由線上中心營運商實施的規則。See Joel R. Reidenberg, “Lex Informatica: The Formulation of Information Policy Rules through Technology,” *Texas Law Review* 76, no. 3 (1997): 553-593.

¹⁵ Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006); Jacqueline D. Lipton, “Law of the Intermediated Information Exchange,” *Florida Law Review* 64 (2012): 1337-1368.

8 區塊鏈與法律：程式碼之治

社會組織結構。

今日，對社會治理焦點施加影響的主要是機構和官僚體系，他們依靠法律和等級制度使社會有序。¹⁶基於區塊鏈的應用不依賴這些規則來實現其功能；相反，他們依靠加密安全法來組織經濟和社會活動。¹⁷

隨著技術的進一步成熟，區塊鏈可能會加速權力的結構性移轉，從由政府當局管理的法律和法規，轉向由去中心化基於區塊鏈網路管理的基於密碼的規則和協議。基於密碼的協議和與它們開發的相關決策，將最終決定這些系統如何工作和塑造我們的交流方式。我們可日益將自己置於「密碼之治」之下一—密碼不受任何一方控制，「密碼之治」可能依照「法律之治」運作，或者不依照法律規定運行。¹⁸

本書將探索區塊鏈技術的新興用途，探討那些被視為的好處和挑戰，及加密安全法的輪廓。我們駁斥這樣的觀點：區塊鏈將導致那些假設，創造它的人們所預期的加密無政府狀態，並概述規範該技術的策略。當互聯網第一次出現時，它激發了無政府狀態和無需法律的觀念。正如約翰·佩瑞·巴洛（John Perry Barlow）在1996年發表的「網路獨立宣言」中所描述的那樣，互聯網最初被視為一個新的世界，在那裡傳統的「財

¹⁶ Lawrence Lessing, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999).

¹⁷ A. Aneesh, “Technologically Coded Authority: The Post-industrial Decline in Bureaucratic Hierarchies,” <https://web.stanford.edu/class/sts175/NewFiles/Algocratic%20Governance.pdf>.

¹⁸ See chapter 2. See also Aneesh Aneesh, *Virtual Migration: The Programming of Globalization* (Durham, NC: Duke University Press, 2006); John Danaher, “The Threat of Algocracy: Reality, Resistance and Accommodation,” *Philosophy and Technology* 29, no. 3 (2016): 245-268.

產、表達、身分、運動和背景的法律概念將不再適用。」¹⁹這個世界居住的是「網路公民（netizens）」，他們依靠去中心化網路來組織和管理自己的事務，不受中央政府的干涉。²⁰

然而，隨著互聯網的成熟，巴洛的願景被視為一個純粹的烏托邦夢想。儘管互聯網最初的設計是為了分散權力，鼓勵通訊自由——即使是以垃圾郵件、詐欺和犯罪為代價——但在過去的十年間，互聯網已經變得日益集中和規範。行動電話、應用商店和雲端運算平臺的出現已經導致一個更集中網路的建立，該網路由少數控制資訊流和經濟交易的公司主導。²¹

今日，互聯網的無政府主義傾向已於相當程度上被馴化了。透過將監管重點集中在互聯網服務供應商（ISPs）和參與創建和部署基於互聯網服務的大型中介機構，各國日益將監管互聯網的任務委託給這些營運商。²²有些國家，特別是在歐洲，甚至開始對互聯網分門別類，實施資訊本地化要求，以防止外國公司收集和儲存有關其公民的資訊。²³中國、俄羅斯、朝鮮和伊朗等國家更進一步，部署國家防火牆，建立一個沒有西方影響或國內異議的網際網路。²⁴

¹⁹ John Perry Barlow, “Declaration of Independence for Cyberspace” (1996), <https://www.eff.org/cyberspace-independence>.

²⁰ Ibid.

²¹ Yochai Benkler, “Degrees of Freedom, Dimensions of Power,” *Daedalus* 145, no. 1 (2016): 18-32; Derek E. Bambauer, “Middlemen,” *Florida Law Review Forum* 64 (2013): 64-67.

²² Lipton, “Law of the Intermediated Information Exchange.”

²³ Anupam Chander and Uyên P Lê, “Data Nationalism,” *Emory Law Journal* 64, no. 3 (2015): 677-739.

²⁴ Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008).

10 區塊鏈與法律：程式碼之治

我們認為區塊鏈技術的增長和發展將遵循相似的路徑。儘管區塊鏈創造出日益自主和潛在的無需法律的系統，但仍然有方法型塑及控制其使用和部署。區塊鏈可能會減少對中央的需求，但不可能完全消除它們。即使區塊鏈導致廣泛去中心化的假設成立，法律、市場力量、社會規範和程式碼本身也可以用來維護法治。

隨著技術的發展並日益被接受，各國政府將有許多工具可供選擇，來塑造或扭曲該技術。他們可以對終端用戶進行管理，對任何透過使用這些系統促進的非法活動，甚至支持基於區塊鏈的應用程式，都要求用戶們承擔責任。或者，除此之外，它們還會對維護這些系統的軟體開發人員、硬體製造商和在TCP/IP堆疊運行較低的中介商施加更大的壓力。

例如，政府可以對互聯網服務供應商和資訊中介機構（如搜索引擎）實施管理，並要求這些中介機構有目的地阻止或避免索引一些非法的基於區塊鏈的應用。他們可以規範支持和維護區塊鏈網路的各方（「礦工」）和提供這些網路運行所需工具的軟體開發商或硬體製造商。對各方的管理，既可以透過對行動者施加規則而直接實現，也可以透過改變其潛在的經濟激勵和收益結構而間接實現。

區塊鏈仍然不夠成熟。因此，各國政府可以透過教育、正式的國際工作組或其他非正式的討論和審議手段，制定與技術相關的新興社會規範。他們還能依靠區塊鏈技術本身來實現特定的政策目標，將某些法律法規編碼至基於區塊鏈的網路及相關的智慧合約中。

本書探討區塊鏈技術的雙重性，描述加密安全法的出現，並概述監管的潛在途徑。我們假設（讀者）不瞭解區塊鏈技術，首先提供區塊鏈的詳細歷史和技術回顧，解釋比特幣和以太坊以及其他相關技術的誕生。再提煉區塊鏈的核心特性，並



解釋為什麼這些特性促進了加密安全法，並將我們推向不斷進步的演算法控制和程式碼之治。最後分析——透過實施加密安全法——區塊鏈如何支持及破壞現有法律，而技術如何準備好在各種背景下影響現有的社會和政治機構，從支付、契約法和金融到資訊、通訊系統或機器對機器的互動。

在描述區塊鏈技術提出（並面臨）的法律挑戰之後，我們概述如何對區塊鏈系統進行監管，以及這樣做的成本。我們以展望未來結束，研究區塊鏈技術如何透過將全部或部分法律轉化為密碼來支持或補充法律，並探究這種監管路徑的危險性。我們的目標是瞭解區塊鏈如何工作、技術的潛在用途、加密安全法的獨特特徵以及監管的潛在途徑。



購書請上：<http://www.angle.com.tw/Book.asp?BKID=10520>

國家圖書館出版品預行編目資料

區塊鏈與法律：程式碼之治／Primavera De Filippi,
Aaron Wright 著；王延川譯。

-- 初版. -- 臺北市：元照，2019. 02
面；公分

譯自：Blockchain and the law: the rule of code
ISBN 978-957-511-076-5（平裝）

1.資訊法規 2.電子貨幣 3.論述分析

312.023

108000058

區塊鏈與法律：程式碼之治

BLOCKCHAIN AND THE LAW: THE RULE OF CODE

5J026RA

2019年2月 初版第1刷

作 者	Primavera De Filippi, Aaron Wright
譯 者	王延川
校 訂	徐珮菱
出 版 者	元照出版有限公司 100 臺北市館前路 28 號 7 樓
網 址	www.angle.com.tw
定 價	新臺幣 450 元
專 線	(02)2375-6688
傳 真	(02)2331-8496
郵政劃撥	19246890 元照出版有限公司

Copyright © by Angle publishing Co., Ltd.

登記證號：局版臺業字第 1531 號

ISBN 978-957-511-076-5

BLOCKCHAIN AND THE LAW: The Rule of Code by Primavera De Filippi and
Aaron Wright

Copyright©2018 by the President and Fellows of Harvard College

Published by arrangement with Harvard University Press through Bardonia-Chinese
Media Agency

Complex Chinese translation copyright©2019

By Angle Publishing Co., Ltd.

ALL RIGHTS RESERVED



元照出版

搶先試閱版

區塊鏈與法律 程式碼之治

Blockchain and the Law: The Rule of Code

本書提出區塊鏈技術所面臨的法律挑戰，研究區塊鏈技術如何透過將全部或部分法律轉化為程式碼來支持或補充法律，並探究這種監管路徑的危險和成本。對於想要瞭解區塊鏈的工作機理、技術的潛在用途、加密安全法的獨特特徵以及監管的潛在途徑的讀者而言，本書堪稱權威之作。

ISBN 978-957-511-076-5



5J026RA

定價：450元



元照網路書店



元照粉絲團



元照出版公司

地址：臺北市館前路28號7樓

電話：(02)2375-6688

網址：www.angle.com.tw